UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/708,402 | 03/01/2004 | Kousik Nandy | CSCO-034 (305764) | 2401 |

86421 7590 10/29/2009

Patent Capital Group - Cisco
6119 McCommas
Dallas, TX 75214

| EXAMINER | |
|---|---|
| JACKSON, JENISE E | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2439 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 10/29/2009 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

thomasframe@patcapgroup.com
patbradford@patcapgroup.com
peggsu@cisco.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/708,402 | NANDY ET AL. | |
| | Examiner | Art Unit | |
| | JENISE E. JACKSON | 2439 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *22 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-75* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-75 are rejected under 35 U.S.C. 102(e) as being anticipated by Bahl et al(2003/0069016).

3. As per claims 1, 18, 34, Bahl et al discloses a method of providing a secure connection from a first end machine(i.e. mobile host) to a second end machine(i.e. correspondent host)(see fig. 2 sheet 2), said method being performed in said first end machine, said method comprising: negotiating a first set of attributes of a security association (SA) with said second end machine[0005, 0032-0033], wherein said first set of attributes are used to provide said secure connection to said second end machine; sending to said second end machine a first packet using said SA, wherein said first end machine is assigned a self address equaling a first address such that said first packet is sent with said first address and using said SA; detecting that said self address is changed to a new address[0040-0043]; sending a request to said second end machine, wherein said new address is contained in a payload portion of a packet forming said request, said request indicating that said self address has changed to said new address; and sending to said second end machine a second packet using said SA, wherein said second packet contains said new address as a source address[0041-0043], wherein the first end machine(i.e. mobile host) is

configured to send an update address request(i.e. address change message) to a gateway providing connectivity to the first end machine[0021, 0024], the update address request indicating the new address is to be bound to the SA, the first end machine(i.e. mobile host) being further configured to receive an acceptance message from the gateway, the acceptance message(i.e. acknowledgement message, 108) signifying that the new address is bound to the SA such that a flow is facilitated by the second machine(i.e. correspondent host) using the SA and using the first set of attributes[0025-0026, 0033, 0041-0043].

4. As per claims 2, 19, 35, 51, Bahl discloses encrypting a portion of said payload containing said new address to generate an encrypted data and including said encrypted data in said request[0043].

5. As per claims 3, 20, 36, 52, Bahl discloses including an authentication data in said payload, wherein said authentication data authenticates that said payload is sent from said first system[0042].

6. As per claims 4, 21, 37, Bahl discloses receiving from said second end machine a third packet in response to said second packet[0049].

7. As per claims 5, 22, 38, Bahl discloses wherein said second packet and said third packet relate to user applications [0030].

8. As per claim 6, Bahl discloses receiving a response from said second end machine, where said response indicates whether said new address is bound to said SA, wherein said second packet is sent after receiving said response[0033, 0038].

9. As per claims 7, 24, 40, Bahl discloses wherein a plurality of secure connections are provided between said first end machine and said second end machine[0005, 0030], wherein a plurality of SAs are present associated with corresponding ones of said plurality of secure connections, said method further comprising: including an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is bound to all of said plurality of SAs in said second end machine[0033, 0043].

10. As per claims 8, 25, 32, 41, 48, 53, 61, Bahl discloses wherein said negotiating is performed according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said new address is contained in an ISAKMP portion of said payload[0033, 0043].

11. As per claim 9, Bahl discloses wherein said packet comprises an IP packet[0043].

12. As per claims 10, 26, 42, Bahl discloses wherein said first end device comprises a client system from which a user accesses a server system[0020].

13. As per claims 11, 27, 43, 49, Bahl discloses a method of providing a secure connection from a first end machine to a second end machine, said method being performed in said second end machine[0005, 0030], said method comprising: negotiating a first set of attributes of a security association (SA) with said first end machine, wherein said first set of attributes are used to provide said secure connection to said first end machine[0005, 0032-0033]; binding said SA to a first address, wherein said first address comprises a self_address of said first end machine; receiving a request indicating that said self_address of said first end machine is changed to a new address, wherein said new address is contained in a payload portion of a packet forming said request; and binding said SA to said new address[0042-0043], wherein the first end machine(i.e.

mobile host) is configured to send an update address request(i.e. address change message) to a gateway providing connectivity to the first end machine[0021, 0024], the update address request indicating the new address is to be bound to the SA, the first end machine(i.e. mobile host) being further configured to receive an acceptance message from the gateway, the acceptance message(i.e. acknowledgement message, 108) signifying that the new address is bound to the SA such that a flow is facilitated by the second machine(i.e. correspondent host) using the SA and using the first set of attributes[0025-0026, 0033, 0041-0043].

14. As per claims 12, 28, 44, Bahl discloses wherein said payload portion is received in an encrypted format, said method further comprising decrypting said payload portion to determine said new address[0031, 0033].

15. As per claims 13, 29, 45, Bahl discloses receiving a first packet from said first end machine, wherein said first packet is received using said first address, wherein said first packet is received before receiving said request; receiving a second packet from said first end machine, wherein said second packet is received using said new address, wherein said second packet is received after receiving said request; and processing said first packet and said second packet using said SA[0032-0033, 0040-0043].

16. As per claim 14, Bahl discloses sending a response to said first end machine upon receiving said request, where said response indicates whether said new address is bound to said SA, wherein said second packet is received after sending said response[0022-0023, 0042].

17. As per claims 15, 31, 47, Bahl discloses wherein a plurality of secure connections are provided between said first end machine and said second end machine, wherein a plurality of

SAs are present associated with corresponding ones of said plurality of secure connections, wherein said request includes an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is bound to all of said plurality of SAs[0005, 0030, 0033, 0043].

18. As per claim 16, Bahl discloses wherein said negotiating is performed according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said request is sent consistent with a format specified by ISAKMP[0030].

19. As per claims 17, 33, Bahl discloses wherein said first end device comprises a gateway[0021].

20. As per claim 23, Bahl discloses sending a request to said second end machine, wherein said request indicates that said self_address has changed to said new address; and receiving a response from said second end machine, where said response indicates whether said new address is bound to said SA, wherein said second packet is sent after receiving said response[0022, 0024, 0030].

21. As per claims 30, 46, Bahl discloses receiving a request from said first end machine, wherein said request indicates that said self-address has changed to said new address; and sending a response to said first end machine, where said response indicates whether said new address is bound to said SA, wherein said second packet is received after sending said response[0032-0033, 0040-0043].

22. As per claim 39, Bahl discloses means for sending a request to said second end machine, wherein said request indicates that said self_address has changed to said new address; and means

for receiving a response from said second end machine, where said response indicates whether said new address is bound to said SA, wherein said second packet is sent after receiving said response[0022, 0024, 0030].

23. As per claim 50, Bahl discloses a networking system comprising: a first end device and a second end device operable to: set up a secure connection between said first end device and said second end device, wherein said SA is bound to a first address in said second end device, wherein said first address comprises a self_address of said first end device, wherein said secure connection is based on a security association (SA); change said self_address of said first end device to a new address; send a request to said second end machine, wherein said new address is contained in a payload portion of a packet forming said request, said request indicating that said self address has changed to said new address; and continue using said SA to provide said secure connection between said first end device and said second end device[0032-0033, 0043], wherein the first end machine(i.e. mobile host) is configured to send an update address request(i.e. address change message) to a gateway providing connectivity to the first end machine[0021, 0024], the update address request indicating the new address is to be bound to the SA, the first end machine(i.e. mobile host) being further configured to receive an acceptance message from the gateway, the acceptance message(i.e. acknowledgement message, 108) signifying that the new address is bound to the SA such that a flow is facilitated by the second machine(i.e. correspondent host) using the SA and using the first set of attributes[0025-0026, 0033, 0041-0043].

24. As per claim 54, Bahl discloses wherein said first end device comprises an address block detecting that said self_address has changed from said first address to said new address, said

address block sending a request to said second end device indicating that said new address is to be bound to said SA[0042-0043].

25. As per claim 55, Bahl discloses wherein said second end device comprises: a memory storing a security association database (SAD) representing binding of SAs to corresponding self_addresses at the other end of security connections, wherein said SAD is modified to indicate that said new address is associated with said SA in response to receiving said request[0032-0033].

26. As per claim 56, Bahl discloses wherein said second end device further comprises: a connection management block negotiating a plurality of attributes with said first end device, wherein said plurality of attributes form said SA, said connection management block receiving said request and modifying said SAD to bind said SA to said new address[0005, 0032].

27. As per claim 57, Bahl discloses wherein said second end device comprises a gateway[0021].

28. As per claim 58, Bahl discloses a first end machine providing a secure connection to a second end machine, said first end machine comprising: a connection management block negotiating a first set of attributes of a security association (SA) with said second end machine[0020, 0032], wherein said first set of attributes are used to provide said secure connection to said second end machine; an address block detecting that a self address of said first end machine is changed from a first address to a new address and sending a request to said second end machine[0042-0043], wherein said new address is contained in a payload of a packet forming said request, said request indicating that said self address has changed to said new

address; and a secure transmission block sending to said second end machine a first packet using said SA, wherein said first end machine is assigned a self address equaling a first address such that said first packet is sent with said first address and using said SA, said secure transmission block sending a second packet using said SA and said new address after said address block detects that said self address is changed to said new address[0041-0043], wherein the first end machine(i.e. mobile host) is configured to send an update address request(i.e. address change message) to a gateway providing connectivity to the first end machine[0021, 0024], the update address request indicating the new address is to be bound to the SA, the first end machine(i.e. mobile host) being further configured to receive an acceptance message from the gateway, the acceptance message(i.e. acknowledgement message, 108) signifying that the new address is bound to the SA such that a flow is facilitated by the second machine(i.e. correspondent host) using the SA and using the first set of attributes[0025-0026, 0033, 0041-0043].

29. As per claim 59, Bahl discloses wherein said address block encrypts a portion of said payload containing said new address to generate an encrypted data and includes said encrypted data in said request[0043].

30. As per claim 60, Bahl discloses wherein said address block includes an authentication data in said payload, wherein said authentication data authenticates that said payload is sent from said first system[0024-0026].

31. As per claim 62, Bahl discloses wherein said secure connection is provided using said SA both before and after said the change of said self_address such that said secure communication can be provided with minimal overhead even if said self_address changes[0043].

32. As per claim 63, Bahl discloses wherein said secure transmission block receives from said second end machine a third packet in response to said second packet[0038, 0041].

33. As per claim 64, Bahl discloses wherein said connection management block sends a request to said second end machine, wherein said request indicates that said self_address has changed to said new address, said connection management block receiving a response from said second end machine, where said response indicates whether said new address is bound to said SA in said second machine, wherein said second packet is sent after receiving said response[0005, 0041-0043].

34. As per claim 65, Bahl discloses wherein a plurality of secure connections are provided between said first end machine and said second end machine, wherein a plurality of SAs are present associated with corresponding ones of said plurality of secure connections, wherein said address block includes an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is bound to all of said plurality of SAs in said second end machine[0005, 0030, 0033, 0043].

35. As per claim 66, Bahl discloses wherein said connection management block operates according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said request is sent consistent with a format specified by ISAKMP[0030-0031].

36. As per claim 67, Bahl discloses wherein at least some of said first set of attributes are contained in an ISAKMP SA[0032-0033].

37. As per claim 68, Bahl discloses a second end machine providing a secure connection to a first end machine, said second end machine comprising: a connection management block

negotiating a first set of attributes of a security association (SA) with said first end machine[0005, 0033], wherein said first set of attributes are used to provide said secure connection to said first end machine; and a memory storing a security association database (SAD) indicating that said SA is bound to a first address, wherein said first address comprises a self_address of said first end machine, wherein said connection management block receives a request indicating that said self_address of said first end machine is changed to a new address, changes said SAD to indicate that said SA is bound to said new address, wherein said new address is contained in a payload portion of a packet forming said request[0041-0043], wherein the first end machine(i.e. mobile host) is configured to send an update address request(i.e. address change message) to a gateway providing connectivity to the first end machine[0021, 0024], the update address request indicating the new address is to be bound to the SA, the first end machine(i.e. mobile host) being further configured to receive an acceptance message from the gateway, the acceptance message(i.e. acknowledgement message, 108) signifying that the new address is bound to the SA such that a flow is facilitated by the second machine(i.e. correspondent host) using the SA and using the first set of attributes[0025-0026, 0033, 0041-0043].

38. As per claim 69, Bahl discloses wherein said payload portion is received in an encrypted format, said connection management block decrypting said payload portion to determine said new address [0031].

39. As per claim 70, Bahl discloses further comprising a secure transmission block receiving a first packet from said first end machine, wherein said first packet is received using said first address, wherein said first packet is received before receiving said request, said secure

transmission block receiving a second packet from said first end machine, wherein said second packet is received using said new address, wherein said second packet is received after receiving said request, wherein said secure transmission block processes said first packet and said second packet using said SA[0005, 0032-0033].

40. As per claim 71, Bahl discloses wherein said connection management block receives a request from said first end machine, wherein said request indicates that said self_address has changed to said new address, said connection management block sending a response to said first end machine after changing said SAD, wherein said response indicates whether said new address is bound to said SA, wherein said second packet is received after sending said response [0005, 0041-0043].

41. As per claim 72, Bahl discloses wherein a plurality of secure connections are provided between said first end machine and said second end machine, wherein a plurality of SAs are present associated with corresponding ones of said plurality of secure connections, wherein said request includes an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is bound to all of said plurality of SAs[0005, 0032-0033].

42. As per claim 73, Bahl discloses wherein said negotiating is performed according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said request is sent consistent with a format specified by ISAKMP[0030].

43. As per claim 74, Bahl discloses wherein at least some of said first set of attributes are contained in an ISAKMP SA[0032-0033].

44. As per claim 75, Bahl discloses wherein said first end device comprises a gateway[0021].

***Response to Amendment***

45. A Non-final rejection was mailed on 2/24/09 in which claims 1-75 were rejected. The Applicant has responded to the non-final action. The Applicant amended all independent claims. Claims 1-75 are pending. Applicant's arguments filed 6/22/09 have been fully considered but they are not persuasive. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

***Final Action***

**46. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JENISE E. JACKSON whose telephone number is (571)272-3791. The examiner can normally be reached on Increased Flex time, but generally in the office M-Fri(8-4:30)..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

October 22, 2009
/J. E. J./
Examiner, Art Unit 2439

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434